

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

UNITED STATES OF AMERICA,

Plaintiff,

vs.

NICHOLAS JAMES MORGAN-
DEROSIER,

Defendant.

Cr. No. 3:22-cr-5-PDW

**DEFENDANT'S REPLY IN
SUPPORT OF MOTION TO
SUPPRESS**

I. Introduction

Defendant, Nicholas James Morgan-Derosier, submits this reply in support of his Motion to Suppress. The search warrant for Mr. Morgan-Derosier's home was invalid on its face because it was not particular and it was overbroad. The warrant permitted the kind of general search prohibited by the Fourth Amendment. Even if the warrant was valid, officers executed the search in an unreasonable and unconstitutional manner. The evidence must be suppressed.

Because many of the issues related to this Motion to Suppress are fact-dependent, Mr. Morgan-Derosier requests an evidentiary hearing.

II. Argument

A. The warrant permitted officers to conduct a “general, exploratory rummaging” of Mr. Morgan-Derosier’s belongings and was, therefore, not particular.

“The particularity requirement prohibits officers ‘from conducting general, exploratory rummaging of a person’s belongings,’ and demands that the warrant be

‘sufficiently definite to enable the searching officers to identify the property authorized to be seized.’” *United States v. Shrum*, — F.4th —, 2023 WL 1841193 at *3 (8th Cir. Feb. 9, 2023) (quoting *United States v. Sigillito*, 759 F.3d 913, 923 (8th Cir. 2014)). A warrant satisfies the particularity requirement when it “plac[es] a specific limitation on the search and enabl[es] officers to identify what property was to be seized.” *Id.* at *4.

The warrant did not place any “specific limitation” on the search here. The identification of the crimes in Exhibit A does not limit the scope of the warrant. The issue here is not that the list of crimes is simply in the wrong place.¹ Instead, it is the expansive language on the face of the warrant. The warrant gives officers permission to search for items which are “evidence of a crime” or “contraband, fruits of crime, or other items illegally possessed.”² This broad “catch-all” clause expands the scope of the warrant beyond those crimes identified in Exhibit A. The catch-all provision swallows the specific crime reference and leaves the warrant totally lacking in particularity. *See United States v. LeBron*, 729 F.2d 533, 536–37 (8th Cir. 1984) (finding clause permitting seizure of “other property, description unknown, for which there exists probable cause to believe it to be stolen” to allow an impermissible general search). Because the list of crimes in Exhibit A is overshadowed by the broad catch-all clause, that list cannot serve as the “limiting principle” to justify the warrant.

¹ See Gov. Br. at 1.

² Exhibit 6.

The warrant here is fundamentally flawed because it authorized a general search. “The chief evil that prompted the framing and adoption of the Fourth Amendment was the ‘indiscriminate searches and seizures’ conducted by the British ‘under the authority of general warrants.’” *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980)). “The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous.” *Id.* at 447. Where searches of physical spaces are often limited by the size of the items searched for, those limits generally do not apply in digital spaces. *Id.* Because the government may try to search every file in a digital space, warrants for computers can quickly become general warrants. *Id.*; *see also United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) (“If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment’s particularity requirement.”).

Searching a hard drive is not akin to searching a sealed package. The United States Supreme Court has already discounted the analogy between a cell phone or other computer and a traditional container, such as a package. *Riley v. California*, 573 U.S. 373, 393–97 (2014). Unlike traditional “packages,” personal computers have immense storage capacity which allows them to serve as phones, “cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, . . . newspapers” and so much more.³ *Id.* at 393. When people

³ In the nine years since the Supreme Court’s decision in *Riley*, the opinion’s description of storage capacity has already become outdated. At that time, the Court explained that the standard capacity for the top-selling smartphone was 16

carry their cell phones, they “keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.” *Id.* at 395. Because of the staggering quantity and quality of information stored on cell phones and other personal computers, conduct that is a reasonable search of a package is no longer reasonable when applied to a computer. *See generally id.* (holding search incident to arrest exception does not permit search of a cell phone).

Here, by permitting officers to delve, unrestricted, into all the data stored on Mr. Morgan-Derosier’s computer devices, the warrant authorized a more invasive search than if it had merely permitted officers to search his entire home for “evidence of a crime” or “contraband, fruits of crime, or other items illegally possessed.” The warrant authorized officers to rummage through all types of electronically stored information, without any requirement that the information be tied to a particular crime or that it be within a reasonably recent period. This is the exact kind of general search the Fourth Amendment intends to prohibit. A warrant that permits a search without limitation is not particular.

gigabytes, with models available up to 64 gigabytes. *Riley*, 573 U.S. at 394. Today, 64 gigabytes represents the low-end of storage available on top-market smartphones. William Antonelli, *How to Decide How Much iPhone Storage You Need*, Business Insider (Sep. 29, 2022, 4:10 pm), <https://www.businessinsider.com/guides/tech/how-much-iphone-storage-do-i-need>. (last accessed Feb. 27, 2023). Now, 128- or 256-gigabyte capacities are standard, and phones are available with capacities up to one terabyte. *Id.* While the Court in 2014 was concerned that a standard, 16-gigabyte cell phone could hold “millions of pages of text, thousands of pictures, or hundreds of videos,” *Riley*, 573 U.S. at 394, standard smartphones today can hold eight or sixteen times as much data.

B. The affidavit's failure to articulate a probable cause nexus between the alleged crimes and the items to be searched cannot be saved by an after-the-fact justification.

The government cannot justify the breadth of the search warrant through information that was not included in the warrant, attachment, or affidavit. The overbreadth doctrine requires there be a nexus between the alleged crime and the places or items to be searched. *United States v. Alexander*, 574 F.3d 484, 490 (8th Cir. 2009). In other words, there must be probable cause for officers to search each item or area permitted by the warrant. *See id.* “When the issuing magistrate relies solely on a supporting affidavit in determining probable cause . . . ‘only that information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause.’” *United States v. Saddler*, 19 F.4th 1035, 1039 (8th Cir. 2021) (quoting *United States v. Roberts*, 975 F.3d 709, 713 (8th Cir. 2020)).

Det. Buzzo’s affidavit did not establish probable cause to search records prior to 15 October 2019 or to search image or video files. The government argues that officers had probable cause to search Mr. Morgan-Derosier’s devices for information that occurred before 15 October 2019, and they had probable cause to search his images and video files.⁴ But these arguments were not presented to the magistrate with the warrant. The affidavit does not explain how records predating the alleged crime were relevant to the investigation. Nor does it explain how photos or videos could be business records. Without these explanations, the warrant failed to

⁴ *See* Gov. Br. at 24, 30.

articulate a connection between the alleged crimes and the files to be searched. The warrant cannot be saved by after-the-fact justifications in the government's brief. The Court cannot look outside the four corners of the affidavit for information to establish the required nexus.

Det. Buzzo's mention of photographs and videos in the same paragraph as business records is not sufficient to establish a probable cause nexus. Det. Buzzo stated, "[c]omputers have also revolutionized the way in which people can access and keep their records[,] including personal, business, and financial documents and information."⁵ He later describes that photos and videos can be collected as digital images. But he does not articulate how those photos can be business or financial records, rather than personal records. He does not explain how photos might be used in the landscaping business. Nor does he articulate any reason to believe that Mr. Morgan-Derosier used photos or videos in that way. Although the government states that "it does not take much imagination to see how" images and videos could be used in landscaping,⁶ their list of possibilities is just that: an exercise of imagination. It is not articulated in the warrant. The warrant failed to draw a probable cause connection between the alleged crimes and Mr. Morgan-Derosier's photos and videos. It is, therefore, overbroad.

Courts consider whether a warrant is valid on a case-specific basis. *See United States v. Fiorito*, 640 F.3d 338, 346 (8th Cir. 2011). There may be cases

⁵ Exhibit 5 at ¶ 17.

⁶ Gov. Br. at 30.

where law enforcement has a legitimate reason to believe that a suspect is using sophisticated computer programs or procedures to hide his conduct. In that kind of case, law enforcement may be justified in searching all computer documents and records for evidence of the crime. But this is not that kind of case. Here, Det. Buzzo knew that Mr. Morgan-Derosier was operating his business in broad daylight. Det. Buzzo had been to a job site, seen Mr. Morgan-Derosier's employees working, and spoken to Mr. Morgan-Derosier. Det. Buzzo knew Mr. Morgan-Derosier believed the judicial order was invalid and that he had a constitutional right to earn a living. There was no reason to believe Mr. Morgan-Derosier was hiding his business records or making files appear like something else. The overly broad nature of this warrant was not necessary for officers to find the evidence of business crimes.

C. Officers abandoned the search for business records to search for evidence of child pornography. This was an unreasonable search.

Whether officers conducted an unreasonable search is a factual dispute. Law enforcement conducts an unreasonable search when officers abandon the search authorized by a warrant to search for other contraband. *United States v. Suing*, 712 F.3d 1209, 1212 (8th Cir. 2013). Here, the evidence is clear that officers abandoned the search for business records.

The evidence demonstrates that officers had abandoned the search for business records when they were at Mr. Morgan-Derosier's home. SA Casetta interviewed three of Mr. Morgan-Derosier's employees/roommates: Julia Anderson,

Blake Thoreson, and Christyan Logan.⁷ Ms. Anderson told SA Casetta that Mr. Morgan-Derosier had raped his nephew.⁸ Mr. Thoreson and Mr. Logan told SA Casetta that Mr. Morgan-Derosier had a thumb drive in a bedroom safe, which included a file called “Boys” and at least one picture of “a younger male.”⁹ SA Casetta then seized multiple storage devices—including a thumb drive—from Mr. Morgan-Derosier’s bedroom safe.¹⁰

Mr. Morgan-Derosier arrived at the scene of the search at approximately 11:03 a.m.¹¹ When he arrived, Det. Buzzo began interviewing him.¹² Approximately 30 minutes later, SA Casetta joined the conversation.¹³ SA Casetta informed Det. Buzzo that they had found “interesting stuff” after interviewing Mr. Morgan-Derosier’s employees.¹⁴ SA Casetta specifically asked Mr. Morgan-Derosier why he had diapers in his bedroom.¹⁵ Officers photographed the diapers with the other relevant evidence.¹⁶ SA Casetta also asked Mr. Morgan-Derosier if officers would find “any weird stuff” on Mr. Morgan-Derosier’s computers or hard drives.¹⁷ When

⁷ Exhibit 12, Casetta Report of Investigation.

⁸ *Id.*

⁹ *Id.*

¹⁰ Exhibit 12; Exhibit 13 – Grand Forks Police Dept. Evidence Inventory and Receipt.

¹¹ Exhibit 14 – audio of interview of Mr. Morgan-Derosier, to be filed conventionally with the Court.

¹² *Id.*

¹³ *Id.* at 29:05.

¹⁴ *Id.* at 29:15.

¹⁵ *Id.* at 29:40.

¹⁶ Exhibit 15 – photos from search.

¹⁷ Exhibit 14 at 30:15.

Mr. Morgan-Derosier stated that he used his computers for business activities, SA Casetta asked him if they had anything “picture related.”¹⁸

Det. Freeman’s involvement also demonstrates that the officers had abandoned the search for business records. Det. Freeman investigated a NCMEC CyberTip in early 2019. At that time, Det. Freeman and HSI Special Agent Michael Arel believed that the tip was mostly likely related to Mr. Morgan-Derosier, rather than his business partner.¹⁹ In July 2020, Det. Freeman received information that Mr. Morgan-Derosier had explicit conversations with Justin Langen.²⁰ Det. Freeman connected “Nick” in Mr. Langen’s chats to the Nicholas Morgan-Derosier implicated by the 2019 CyberTip.

Considering the totality of the evidence, it is clear officers were looking for child pornography and not business records. First, SA Casetta’s involvement in a warrant for these state crimes is evidence officers were investigating beyond the scope of the warrant. While some conduct may constitute both federal and state crimes, the crimes named in Attachment A were purely state crimes. Even if potentially federal crimes, they did not implicate HSI’s transnational and national security focus. Child exploitation, in contrast, is routinely investigated by HSI. Second, based on the statements from Mr. Morgan-Derosier’s employees, SA Casetta had a suspicion there could be evidence of child pornography on a thumb

¹⁸ Exhibit 14 at 32:20.

¹⁹ Exhibit 16, email from Michael Arel. “Looks like Nicholas is probably our guy. . . . It would be nice to dump his phone!”

²⁰ Gov Br. at 11.

drive in Mr. Morgan-Derosier's bedroom safe. He promptly seized the thumb drive from the bedroom safe, and it was the first item that Det. Freeman searched. She searched the thumb drive even before she searched the home office computer Mr. Morgan-Derosier had used to operate QuickBooks. Third, SA Casetta asked Mr. Morgan-Derosier about the diapers in his bedroom and whether there would be "any weird stuff" on Mr. Morgan-Derosier's computers. From the context of the interview, it is clear SA Casetta was investigating crimes that were more taboo than the offenses listed in Attachment A — namely, contractor license required, construction fraud, and violation of a judicial order. Fourth, two prior child pornography investigations into Mr. Morgan-Derosier had failed to generate probable cause. The prior failed investigations gave officers a motive to find any reason to get into Mr. Morgan-Derosier's computers. The reason they found was his alleged business crimes. And although the warrant allowed them to search for evidence of those business crimes, they quickly abandoned that search to look for evidence of child pornography.

The government argues that Det. Freeman could only have abandoned her search if she knew the files she opened were not business records.²¹ But an officer does not have to know for certain that her search will reveal contraband to violate the Fourth Amendment's reasonableness requirement. Her behavior becomes unconstitutional when she conducts the unreasonable search, whether that search is fruitful or not. *Cf. United States v. Loera*, 923 F.3d 907, 923 (10th Cir. 2019)

²¹ Gov. Br. at 33.

(finding search unreasonable when officer viewed CDs explicitly to search for child pornography even though warrant permitted search for evidence of computer fraud). “Rather than navigate away from the child pornography,” Det. Freeman “explicitly navigated toward” evidence she knew was not responsive to the warrant. *See id.* at 923. It is the search— i.e. the navigation itself—that was unreasonable. Therefore, her search was unconstitutional.

III. Conclusion

Computers and “cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life.” *Riley*, 573 U.S. at 403 (quotations omitted). When officers seek warrants for these devices, they must meet the standards of particularity and breadth. The warrant here did not meet these standards because it was not limited and because it lacked a probable cause nexus between the alleged crimes and the items to be searched. Additionally, officers executed the warrant unreasonably by abandoning their search for business records. Instead, they quickly began to search for the evidence they were really after: evidence of child pornography.

Because the warrant was invalid on its face and executed unreasonably, the evidence was obtained unconstitutionally. The evidence must be suppressed.

Dated this 27th day of February, 2023.

Respectfully submitted,

JASON J. TUPMAN
Federal Public Defender
By:

/s/ Christopher P. Bellmore
Christopher P. Bellmore
Anne M. Carter
Assistant Federal Public Defenders
Attorneys for Defendant
Office of the Federal Public Defender
Districts of South Dakota and North Dakota
112 Roberts Street North, Suite 200
Fargo, ND 58102
Telephone: 701-239-5111; Facsimile: 701-239-5098
Email: filinguser_SDND@fd.org